IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SEALED

UNITED STATES OF AMERICA

v.

AMECHI COLVIS AMUEGBUNAM

NO. 3-15MJ266-BH

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

From on or about November 5, 2013 through in or about April 24, 2015, in the Dallas Division of the Northern District of Texas and elsewhere, defendant **AMECHI COLVIS AMUEGBUNAM**, and others known and unknown, did knowingly and willfully combine, conspire, confederate, and agree with each other, to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, transmitted and caused to be transmitted by means of wire communication in interstate or foreign commerce, any writings, signs, signals, pictures, and sounds in violation of 18 U.S.C. § 1343.

In violation of 18 U.S.C. § 1349.

This criminal complaint is based on the facts set out in the attached affidavit.

Kathryn Sherman
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence in Dallas, Texas, on April 23, 2015

IRMA C. RAMIREZ
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

1. I make this affidavit in support of a criminal complaint and the issuance of an arrest warrant for **Amechi Colvis Amuegbunam**. This affidavit is made in support of a criminal complaint under 18 U.S.C. § 1349, conspiracy to commit wire fraud (18 U.S.C. § 1343).

2. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since October of 2010. Prior to becoming a Special Agent, I worked with the Department of State in Computer Investigations and Forensics Division. I have a Bachelors of Science degree in Finance and a Bachelors of Arts degree in Criminology. I also have a Masters degree in High Technology Crime Investigations. As a federal agent, I am authorized to investigate violations of Unites States laws and to execute warrant issued under the authority if the Unites States. I am currently assigned to the Dallas Division of the FBI, where I have been tasked to investigate computer crimes.

3. Through information provided to the FBI Dallas Division, the FBI Dallas Cyber Task Force is investigating an extensive money laundering and wire fraud scheme primarily operated by individuals in Nigeria who are exploiting open source information and using social engineering techniques to fraudulently steal millions of dollars from United States corporations and individuals. The individuals in Nigeria are aided and abetted by individuals in the Unites States. This scheme has become so common, that the private sector has described the criminal conduct by coining the phrase "The Business

E-mail Compromise" scheme. The scheme will be hereafter referred to as the BEC scheme.

4. This affidavit is being submitted for the limited purpose of securing an arrest warrant for **Amechi Colvis Amuegbunam**, one of the coconspirators in this investigation. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts, I believe are necessary to establish probable cause to believe that an arrest warrant should be issued for **Amechi Colvis Amuegbunam** based on his violation of 18 U.S.C. § 1349 (18 U.S.C. § 1343).

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. § 2703(a), (b)(1)(A) and (c)(1)(A). Also, this Court is "a district court of the Unites States (including a magistrate judge of such a court) that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

APPLICABLE STATUES and DEFINITIONS

6. There is probable cause to believe that the subject, **Amechi Colvis Amuegbunam**, has conspired to commit wire fraud, in violation of 18 U.S.C. § 1349 (18 U.S.C. § 1343). Section 1349 provides as follows:

> Any person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

7. The elements of a violation of 18 U.S.C. § 1349 are:

First: **Amechi Colvis Amuegbunam** and at least one other person made an agreement to commit the offense of wire fraud in violation of 18 U.S.C. § 1343; and

Second: **Amechi Colvis Amuegbunam** knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose.

8. Title 18 U.S.C. § 1343 provides as follows:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

9. The elements of a violation of 18 U.S.C. § 1343 are:

First: The defendant knowingly created a scheme or artifice to defraud, that is, to obtain money or property by means of false or fraudulent pretenses, representations, or promises, as charged in Count One of the Indictment;

Second: The defendant acted with a specific intent to defraud;

Third: The defendant used interstate wire communications facilities or caused another person to use interstate wire communications facilities for the purpose of carrying out the scheme; and

Fourth: The scheme to defraud employed false material representations.

10. Definitions:

a. Internet Protocol Address: or "IP address" refers to a unique number used by a computer to access the internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

b. Domain name: are common, easy to remember names associated with an IP address. For example, a domain name www.usdoj.gov refers to the IP address 149.101.1.32. Domain names are typical strings of alphanumeric characters, with each level delimited by a period.

FACTS DEMONSTRATING PROBABLE CAUSE

11. The investigation of this BEC scheme was initiated in November of 2013 when two United States companies in the Dallas/Fort Worth area (one in the Northern District of Texas (NDTX) and one in the Eastern District of Texas (EDTX)) reported to the FBI Dallas office that they had received targeted spear phishing e-mails. The targeted spear phishing e-mail received by each company appeared to be a forwarded message allegedly from a top executive at the company, such as the company president, owner, or chief executive or financial officer. The spear phishing e-mail was sent to an employee in the accounting department who had the authority to make financial transfers for the company. Although the e-mail appeared to be coming from the company executive, the message was actually coming from a false e-mail account fraudulently created to look like a legitimate company e-mail account. After complying with the spear phishing e-mails instructions to transfer funds, the companies became victims of the BEC scheme, each losing approximately $100,000.00.

12. As of the date of this Criminal Complaint, Dallas FBI has identified seventeen victim-companies in the Dallas/Fort Worth area (thirteen in the NDTX and four in the EDTX).

13. The perpetrators of this scheme utilize different techniques to gain funds and often use or share the same bank accounts. In addition, the FBI's Internet Crimes Complaint

Center (IC3) has been tracking this scheme. To date, perpetrators of the scheme have victimized over 4000 Unites States based businesses and over 1000 foreign based businesses. The total loss to the United States victims is approximately $350,000,000.00.

14. The BEC scheme begins with a well-worded and targeted spear phishing e-mail. For example, a company's e-mail address may be "abc-company.com." To perpetrate this scheme, the perpetrators register the domain "abc-compnay" (deceptive portion is underlined). The fraudulent domain contained one small difference from the true company's e-mail address (the "n" and the "a" were reversed). The e-mail message was well-worded and directed a company employee in the accounting department to wire a large sum of money to a specific bank account. A PDF document attached to the e-mail contained bank account details and wiring instructions. The e-mail appeared to be from a company executive. In most cases, the company employees who received the e-mail did not recognize the error in the fraudulent domain name and wired the money as instructed.

15. The following e-mail was an actual e-mail used in this spear phishing BEC scheme. (The names on the e-mails were changed by the government to conceal the identity of the employees of the victim company).

> From: Robert Frank ,robert.frank@lumniant.com.
> Sent: Wednesday, November 06, 2013 11:35AM
> To: Holden, Tim
> Subject: Fwd: Wire Instructions
> Attachments: CFC CLEANING & SECURITY SERVICE LIMITED WIRE INSTRUCTIONS.PDF
>
> Tim,
>
> Process a wire of $98,550.00 to the attached account information. Mac will provide me the necessary paperwork later. Code it to Misc. Expense-executive.

> Send me the confirmation when done.
>
> Thanks,
>
> Rob
>
> ----------Forwarded message----------
> From: Mac Myers mac.myers@luminant.com
> Date: Nov 06, 2013
> Subject: Wire Instructions
> To: Robert.Frank@luminant.com
>
> Rob,
>
> Per our conversation, here is the wire transfer instructions for the wire transfer. Let me know when the wire is completed.
>
> Mac

16. The e-mail described above was sent to an employee of Company A an electric utility company headquartered in Dallas, Texas. Luminant Corporation is a subsidiary of Company A The e-mail domain name used by Luminant Corporation employees is Luminant.com.

17. Company A wire transferred $98,550.00 from its account at a bank in the NDTX to a bank outside the state of Texas, as directed in the PDF, resulting in a financial loss to Company A.

18. The message from **robert.frank@lumniant.com** to Tim Holden was fraudulently drafted to look like an e-mail sent from the company's Senior Vice President, Robert Frank. The perpetrator used the names of the actual employees of the company, with what appeared to be actual e-mail addresses. However, the real domain for the victim company was @luminant.com. The fraudulent domain interchanged the letters "n" and "i" in the domain name.

19. A WHOIS lookup showed that the domain associated with the spear phishing e-mail, **lumniant.com**, had been registered at Vistaprint. The Dallas FBI received subpoena results from Vistaprint on January 29, 2014, for the domain **lumniant.com**. The domain **lumniant.com** was registered on November 6, 2013, along with thirty other domains. All of these domains were registered between 10:30 and 10:45 EST and the IP address used to register the domains was 75.125.151.194.

20. The Dallas FBI also analyzed the e-mail header information which showed that the e-mail described in paragraph 15 was sent from IP address 75.125.151.194 on November 6, 2013, at 11:35 AM (time zone unknown).

21. Lastly, the Dallas FBI analyzed the metadata of the PDF file that was attached to the e-mail, "CFC CLEANING & SECURITY SERVICE LIMITED WIRE INSTRUCTIONS.PDF." The metadata showed that the document was created on a Mac OS X 10.8.5 Quartz on November 5, 2013, at 4:26pm and the author of the document was "Colvis Amue." At the

REDACTED

REDACTED

22. A second victim in the NDTX is [Company B (**B**)]. On May 16, 2014, (The names on the e-mails were changed by the government to conceal the identity of the employees of the victim company) Steven Smith, Controller at [**B**] received an e-mail from what appeared to be the Chief Financial Officer from an e-mail displaying the domain @[Company B].com. The company's legitimate e-mail domain is [Company B]com. The fraudulent domain is missing the "r" in energy.

23. Smith, not knowing that the e-mail was fraudulent, wire transferred $370,455.12 from its account at a bank in the NDTX to a bank outside the state of Texas, as directed in the PDF, resulting in a financial loss to [**B**]

24. Affiant examined the PDF document titled, "GREEN EMPIRE VENTURES WIRE INSTRUCTIONS.PDF." The metadata of this PDF showed that the document was created on a Mac OS X 10.8.5 on May 15, 2014, at 3:51pm, and the author of the document was "**Colvis Amue**". To the left is a

REDACTED

REDACTED

25. Again on May 19, 2014, [**B**] received a second e-mail directing that $274, 309.12 be sent to an account outside the state of Texas, as identified in the attached PDF. [**B**] recognized that the second e-mail was fraudulent and did not send the funds as directed.

26. The PDF document, which was attached to the second e-mail was titled, "APEX BASIC LTD WIRE INSTRUCTIONS.PDF." The metadata of this PDF showed that the document was created on a Mac OS X 10.8.5 on May 19, 2014, at 2:12pm, and the author of the document was "**Colvis Amue**". To

REDACTED

REDACTED

27. According to information received from Vistaprint, the domain Company B R.COM was registered on May 16, 2014, at 11:58 EST from IP address 75.125.151.194. This domain was cancelled on May 17, 2014. The same domain was re-registered at Vistaprint on May 19, 2014, at 12:13:23 EST from IP address 108.59.8.131.

28. As it relates to **Amechi Colvis Amuegbunam,** the BEC scheme was attempted with two companies in the EDTX. One company wire transferred $146,550.00 from its account at a bank in the EDTX to a bank outside the state of Texas, as directed in the PDF attached to the fraudulent e-mail, resulting in a financial loss to that company. The second company realized the e-mail was fraudulent and did not send the $381,903.22 as directed in the attached PDF. Affiant examined the PDF documents attached to both e-

mails. The metadata showed that the PDF documents attached to both emails were created by "Colvis Amue."

29. The Dallas FBI quickly learned that this was a wide spread scheme. IC3 provided additional victim companies to the Dallas FBI that were located throughout the United States.

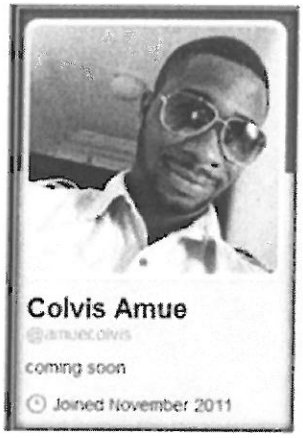
30. Dallas FBI was able to determine that the same BEC scheme is being perpetuated by multiple individuals. The Dallas FBI office and the FBI Cyber Division's Cyber Initiative and Resource Fusion Unit (CIRFU) have examined the metadata from hundreds of PDF documents that were sent to U.S. and international companies in an effort to further the BEC scheme.

31. The metadata has identified seventeen (17) different users were creating the PDF documents. Dallas FBI has identified the true identity of six (6) of those individuals, who are considered subjects of the Dallas investigation. One of which is **Amechi Colvis Amuegbunam**. CIRFU has identified "**Colvis Amue**" as the creator of eight (8) additional PDF documents that were sent to various companies in the United States. The attempted loss for these companies is approximately $500,000.00. (Note: To date, CIRFU is still going through data and analyzing the PDF documents. It is likely that "**Colvis Amue**" will be identified as the author of additional PDF documents).

32. Based on the incidents described in this affidavit (the 5 incidents in the NDTX and EDTX) and the 8 additional incidents discovered by CIRFU, **Amechi Colvis Amuegbunam** is responsible for over a $1.3 million dollar attempted loss and $615,555.00 actual loss to U.S. companies.

Identifying "Colvis Amue" as Amechi Colvis Amuegbunam

33. As described above, "Colvis Amue" was shown to be the author of the PDF documents attached to BEC scheme e-mails sent to U.S. companies. An open source search for "**Colvis Amue**" identified a Twitter account with the user name



"**@amuecolvis**" and an Instagram account with the user name "**aacolvis**." Affiant has examined the photographs posted to each account and verified they are the same person. As an example, the photograph to the left was uploaded to both the **@amuecolvis** Twitter account and the **aacolvis** Instagram account.

34. On February 11, 2014, subpoena return information from Twitter showed that the e-mail address used to create the **@amuecolvis** account was **aamue**@yahoo.com

35. On March 18, 2015, Dallas FBI obtained search warrant data from Instagram for the account **aacolvis**. The e-mail address used to create this account was **colvis_amechi**@yahoo.com.

36. On January 24, 2015, **Amechi Colvis Amuegbunam** entered the United States at

JFK International Airport in New York, NY. On **Amechi Colvis Amuegbunam** NIV applicant details paperwork, he listed his e-mail address as **aamue**@yahoo.com. **Amechi Colvis Amuegbunam** entered the country with a Nigerian passport containing the photo for **Amechi Colvis Amuegbunam** (see left).

Affiant was advised that **Amechi Colvis Amuegbunam** is here on a two (2) year student visa. His passport provided the following information:

Full Name: **Amechi Colvis Amuegbunam**
Sex: Male
DOB: 1987
POB: Lagos, Nigeria
Nationality: Nigerian
Citizenship: Nigeria

37. This photo matches the individual seen in the photographs posted to the **@amuecolvis** Twitter account and the **aacolvis** Instagram account.

Coconspirators

38. As discussed in paragraph 31, Dallas FBI has identified a total of 6 individuals who created the PDF documents used in the BEC scheme, one of which is **Amechi Colvis Amuegbunam.** The metadata of the PDFs provided a nickname for the remaining

REDACTED

REDACTED

40. These five (5) additional coconspirators are all located in Lagos, Nigeria. They will not be named or charged at this time in that the investigation is ongoing.

41. In addition to being connected on social media, the coconspirators also used the same information and computer systems (as seen in the document properties for the PDFs) to further the BEC scheme.

42. As described in paragraphs 19, 20, and 28, the IP address 75.125.151.194 was frequently used to register domains at Vistaprint and to send BEC e-mails to victim companies.

43. On December 17, 2013, Dallas FBI received subpoena results from Hosting Services Inc., for IP address 75.125.151.194. The results showed that this IP address is registered to Amplusnet SRL in Tg. Mures, Romania. Dallas FBI sent a Mutual Legal Assistance Treaty request to Romania requesting subscriber information for this IP address and a second IP address that was frequently used in the same capacity. In January 2015, the Dallas FBI received the subscriber information from Amplusnet SRL. The registration information showed that one of the five unidentified coconspirators was the registrar for this IP address with the Romanian internet service provider, Amplusnet SRL.

44. Lastly, the Dallas FBI has documented all of the bank accounts listed in the attached PDF documents. The bank account information has been for accounts in the United States and other countries. **Amechi Colvis Amuegbunam** and the five (5) identified coconspirators used the same bank accounts and the same money mules to facilitate the wire transfers.

REQUEST FOR SEALING

45. The information in this affidavit describes an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. While the government has identified 6 coconspirators, there are more that have not been identified. Therefore, there is good cause to seal these documents because their premature disclosure may give the targets of the investigation an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change pattern of behavior, notify confederates, or otherwise seriously jeopardize the investigation. Accordingly, I respectfully request that all papers in support of this application be sealed until further order of Court, except as necessary to facilitate the execution of the arrest warrant.

Conclusion

46. Based on the foregoing specific and articulable facts, there is probable cause to believe that **Amechi Colvis Amuegbunam** has conspired with other to commit wire fraud, in violation of 18 U.S.C. § 1349 (18 U.S.C. § 1343), and that a warrant should be issued for his arrest.

Kathryn Sherman
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me on April 23, 2015.

IRMA C. RAMIREZ
United States Magistrate Judge